



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,522	07/02/2003	Liqun Chen	B-5153 621074-2	4783
<div>7590 09/20/2007 HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400</div>			<div>EXAMINER ABEDIN, SHANTO</div>	
			<div>ART UNIT 2136</div>	<div>PAPER NUMBER</div>
			<div>MAIL DATE 09/20/2007</div>	<div>DELIVERY MODE PAPER</div>

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/613,522	Applicant(s) CHEN ET AL.	
	Examiner Shanto M Z Abedin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 June 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17, 19-25, 27 and 28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17, 19-25, 27 and 28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in response to the communication filed on 06/26/2007.
2. Claims 1-17, 19-25, 27-28 are currently presented for the examination.
3. Claims 1-17, 19-25, 27-28 have been rejected.

Response to Arguments

4. The applicant's argument's regarding the previous 35 USC 101 rejections are fully considered, however, found not persuasive. The previous 35 USC 101 rejections of claims 1-5 are withdrawn due to the amendments made to the independent claim. The previous 35 USC 101 rejections of claims 12-17, 25 and 27-28 are maintained (please see the office action below for detail).
5. Regarding the previous 35 USC 102 (e) rejection of claims 1-17, 19-25, 27-28, the applicant primarily argues that the reference Gentry et al'554 does not teach or suggest:
 - (a) computing first, second and third verification parameters as the product of second secret with said shared secret, the second element and the first element respectively;
 - (b) outputting the first, second and third verification parameters for use by the third party in proving the association between the first and second parties.

© carrying out a first check: $p(\text{third verification parameter, computed second element}) = p(\text{first element, second verification parameter})$; and

carrying out a second check: $p(\text{first element, first verification parameter}) = p(\text{first product, second verification parameter})$.

In response to the above argument (a), it is fully considered, however, found not persuasive since upon further consideration Gentry et al'554 was found to teach these limitations (please see the office action below).

In response to the above arguments (b) and (c), they have been considered but are moot in view of the new ground(s) of rejection (please see the office action below). Furthermore, in response to applicant's arguments (b) regarding claims 6 and 8, the recitation "third party...carrying out" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 12-17, 25, and 27-28 are rejected under 35 U.S.C. §101 because claimed invention as a whole either fails to accomplish a practical/ useful end result, or directed to a program per se product.

Regarding claims 12-17, the features and the elements of the claims merely represent an abstract/ mathematical idea, or manipulation of abstract/ mathematical idea – they lack producing

required useful/ practical results at the end. Therefore, the claims are non statutory under 35 U.S.C. 101 as not being useful (MPEP § 2106).

Regarding claim 25, the features and the elements of the claims merely discloses an hierarchy of trusted authorities – they lack producing required useful/ practical results at the end. Therefore, the claims are non statutory under 35 U.S.C. 101 as not being useful ((MPEP § 2106).

Regarding claims 27-28, they are rejected as being non statutory since they disclose only non function data, or a computer program per se product. A computer program product merely stored in a computer readable media is non-statutory (MPEP § 2106.01 [R-5]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-17, 19-25, 27-28 are rejected under 35 USC 103 (a) as being unpatentable over Gentry et al' 554 (US 2003/ 0182554 A1) in view of Boneh et al (US 2003/0081785A1) further in view of Gentry et al' 885 (US 2003/0179885A1).

Regarding claims 1 and 27, Gentry et al '554 discloses a method/ computer program product of enabling a third party to verify an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group, formed from an identifier string of the second party using a hash function, and there being a

computable bilinear map for the first and second elements; wherein a second party computer entity, acting on behalf of the second party:

receives a shared secret provided by the first party as the product of a first secret and the second element (Fig 1,5; Par [0011], [0019], [0024]; receiving first intermediate shared secret elements/ component from the first entity);

computes first ([0033]; interactive shared secret), second ([0024];second intermediate shared secret component)and third (first intermediate shared secret component) verification parameters as the product of a second secret with said shared secret ([0022]-[0024]; non-interactive shared secret) , the second element and the first element ([0024]-[0025]; first and second random secret) respectively.

outputs the first, second and third verification parameters (Par [0022]-[0025], [0033]; outputting interactive shared secret, second and first intermediate shared secret components).

Gentry et al '554 fails to disclose expressly

the first, second and third verification parameters for use by the third party in proving the association between the first and second parties .

however, Boneh et al discloses the first, second and third verification parameters for use by the third party in proving the association between the first and second parties (Par [0053]-[0063]; claims 36-38; PKG conducting authentication based on parameter, master key, and ID).

Furthermore, Gentry et al' 885 discloses the first, second and third verification parameters for use by the third party in proving the association between the first and second parties (Par [0049]-[0053]; [0085], [0135]-[0140]; Claims 15-40, 56-65).

Gentry et al' 885 , Boneh et al and Gentry et al '554 are analogous art because they are from the same field of authentication based on identity and bilinear mapping . At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teaching of Boneh et al and Gentry et al' 885 with Gentry et al '554 to use the first, second and third verification parameters for use by the third party in proving the association between the first and second parties in order to provide a alternative third party authentication .

Regarding claims 8, 22 and 28, they are rejected applying as above rejecting claim 1, furthermore, Gentry et al '554 discloses a method/ apparatus/ computer program product of verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group; the first and second elements being such that there exists a bilinear mapping p for these elements; the method comprising a third party computer entity carrying out the following operations:

receiving data indicative of said first element, and a first product formed by the first party from a first secret and the first element (Par [0011], [0019], [0022]-[0024]; first and second secret elements; PKG knowing secret components and private keys);

receiving in respect of the second party both an identifier string, and first, second and third verification parameters (Par [0022], [0022]-[0024]; Claim 1; first and second secrets and system parameter; PKG knowing secret components and private keys);

computing the second element from the identifier string of the second party (Par [0022]);

carrying out a first check: $p(\text{third verification parameter, computed second element}) = p(\text{first element, second verification parameter})$ (Par [0028]- [0034], Claim 11, 18, 19; determining and checking first MAC)

carrying out a second check: $p(\text{first element, first verification parameter}) = p(\text{first product, second verification parameter})$ (Par [0028]- [0034], Claim 11, 18, 19; determining and checking second MAC)

the association between the first and second parties being treated as verified if both checks are passed (Par [0028, [0033]; Claim 19; authentication).

Gentry et al '554 fails to disclose a third party computer entity carrying out the above checking operations.

However, Boneh et al discloses a third party carrying out a first check: $p(\text{third verification parameter, computed second element}) = p(\text{first element, second verification parameter})$ (Par [0053]- [0063]; claims 36-38; PKG conducting authentication based on parameter, master key, and ID)

carrying out a second check: $p(\text{first element, first verification parameter}) = p(\text{first product, second verification parameter})$ (Par [0053]-[0063]; claims 36-38; PKG conducting authentication based on parameter, master key, and ID)

the association between the first and second parties being treated as verified if both checks are passed (Par [0053]-[0063]; claims 36-38; PKG conducting authentication based on parameter, master key, and ID).

Furthermore, Gentry et al' 885 discloses receiving in respect of the second party both an identifier string, and first, second and third verification parameters (Par [0049]-[0053]; [0085], [0135]-[0140]; Claims 15-40, 56-65); and

a third party carrying out a first check: p (third verification parameter, computed second element) $= p$ (first element, second verification parameter) (Par [0049]-[0053]; [0085], [0135]-[0140]; Claims 15-40, 56-65; PKG / root carrying out and comparing signatures/ hash functions, H)

carrying out a second check: p (first element, first verification parameter) $= p$ (first product, second verification parameter) (Par [0049]-[0053]; [0085], [0135]-[0140]; Claims 15-40, 56-65; PKG / root carrying out and comparing signatures/ hash functions, H)

the association between the first and second parties being treated as verified if both checks are passed (Par [0049]-[0053]; [0085], [0135]-[0140]; Claims 15-40, 56-65; PKG / root carrying out and comparing signatures/ hash functions, H for authentication).

Regarding claim 12, Gentry et al '554 discloses method of enabling verification of an association between parties, the method comprising:

generating a first private key and public key for a first party (par [0003], [0022]; generating private, public keys);

generating a second private and public key for a second party wherein the second private key is derived from the first private key and second public key (par [0003], [0022]); and

generating a third private key for the second party that is used in association with the first public key, the second private key and the second public key to form a first cryptographic parameter, a second cryptographic parameter and a third public key respectively (Par [0022], Claim 6,12; private, public keys; first and second secrets).

outputting the first, second, and third cryptographic parameters (Par [0022]-[0025], [0033]; outputting interactive shared secret, second and first intermediate shared secret components).

Regarding claim 19, it recites the limitations of claim 1, therefore, it is rejected applying as above rejecting claim 1, furthermore, Gentry et al '554 discloses apparatus arranged to enable a third party to verify an association between the apparatus and a first party that has a first secret and is associated with a first element of a first algebraic group, the apparatus being associated with a second element, of a second algebraic group, and the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

a memory for holding a second secret and an identifier string associated with the apparatus (Par [0010], Claim 18, 19; memory),

means for forming said second element from said identifier string using a hash function (Par [0041]; Claim 18, 19; processor),

means for receiving from the first party a shared secret based on said first secret and said first element, and for storing this shared secret in the memory (Claim 1,6,18; entity; communicating),

means for computing first, second and third verification parameters as the product of the second secret with said shared secret, said second element and said first element respectively (Par [0041]; Claim 18, 19; processor).

Gentry et al '554 fails to disclose expressly means for making available said identifier string and said verification parameters to the third party.

However, Boneh et al discloses means for making available said identifier string and said verification parameters to the third party (Par [0053]-[0063]; claims 36-38; PKG knowing and receiving secrets and components).

Regarding claim 25, it is rejected applying same motivation and rationale rejecting claim 1, furthermore, Gentry et al '554 discloses a hierarchy of trusted authorities wherein:

each trusted authority is associated with a point on an elliptic curve, this point being derived, at least for each non-root trusted authority, from an identifier string of the trusted authority (Par [0003], [0004]; deriving keys from master secret; trusted party);

trusted authorities each has a standard elliptic-curve public/private key pair wherein the private key is formed by a secret of the trusted authority concerned and the public key comprises the product of this secret with the point associated with that trusted authority (Par [0003], [0004]; claim 6-7; elliptic curve; shared secret);

trusted authorities each has an identifier-based elliptic-curve public/private key pair wherein the public key comprises the identifier string of the trusted authority concerned and the private key is a shared secret provided by a said trusted authority at a next level up in the hierarchy, the shared secret being the product of the secret of the next-level-up trusted authority and the point associated with the trusted authority to which the shared secret is provided (Par [0021], [0022], [0040]; Claim 18, 19; root level/ master secret; authentication; trusted party); and

authorities each has two further public parameters formed by the product of the secret of the trusted authority respectively with the shared secret provided to it by the next-level-up trusted authority and with the point associated with the latter (Par [0021], [0040]; Claims 1-3, 18, 19; determining first, second intermediate shared secret, and interactive shared secret).

Gentry et al '554 fails to disclose hierarchy of trusted authorities including non-leaf trusted authorities, and non-root trusted authorities.

However, Gentry et al' 885 discloses hierarchy of trusted authorities including non-leaf trusted authorities, and non-root trusted authorities (Fig 3).

Regarding claim 2, Boneh et al discloses method a wherein the second party generates a further shared secret from the second secret and an identifier string of a fourth party, the second party passing this further shared secret to the fourth party for use by the latter as the private key of a public/private key pair the public key of which is formed by the identifier string of the fourth party (Par [0053]-[0063]; association between multiple parties based on plurality of ID's and private keys).

Regarding claim 3, Gentry et al '554discloses a method wherein the first and second parties are respectively parent and child trusted authorities in a hierarchy of trusted authorities (Par [0003], [0004]; trusted party).

Regarding claim 4, Gentry et al '554discloses a method wherein the first and second algebraic groups are the same (Par [0019]; algebraic groups).

Regarding claim 5, Gentry et al '554discloses a method wherein the first and second elements are points on the same elliptic curve (Par [0019]; elliptic curves).

Regarding claim 6, Gentry et al '554discloses method of verifying an association between the first and second parties of claim 1 by using a function p providing said bilinear map; the method

comprising a third party computer entity carrying out the following operations using the verification parameter of claim 1:

computing the second element from the identifier string of the second party (Par [0022]);

carrying out a first check: $p(\text{third verification parameter, computed second element}) = p(\text{first element, second verification parameter})$ (Par [0028]- [0034], Claim 11, 18, 19; determining and checking first MAC)

carrying out a second check: $p(\text{first element, first verification parameter}) = p(\text{first product, second verification parameter})$ (Par [0028]- [0034], Claim 11, 18, 19; determining and checking second MAC)

the association between the first and second parties being treated as verified if both checks are passed (Par [0028, [0033]; Claim 19; authentication).

Gentry et al '554 fails to disclose a third party computer entity carrying out the above checking operations. However, Boneh et al discloses a third party carrying out a first check: $p(\text{third verification parameter, computed second element}) = p(\text{first element, second verification parameter})$ (Par [0053]-[0063]; claims 36-38; PKG conducting authentication based on parameter, master key, and ID)

carrying out a second check: $p(\text{first element, first verification parameter}) = p(\text{first product, second verification parameter})$ (Par [0053]-[0063]; claims 36-38; PKG conducting authentication based on parameter, master key, and ID)

the association between the first and second parties being treated as verified if both checks are passed (Par [0053]-[0063]; claims 36-38; PKG conducting authentication based on parameter, master key, and ID).

Regarding claim 7, Gentry et al '554discloses the method wherein said bilinear mapping function is based on a Tate or Weil pairing (Par [0021]; Tate or Weil pairing).

Regarding claim 9-11, they recite the limitations of claims 4-5 and 8, therefore, they are rejected applying as above rejecting claims 4-5 and 8.

Regarding claim 13, Gentry et al '554discloses the method wherein a third party uses the first, second and third cryptographic parameters together with the first and second public keys to check, by using bilinear mapping, whether there is an association between the first and second parties (Par [0022], Claim 6,12).

Regarding claim 14, Gentry et al '554discloses the method wherein the bilinear mapping is based on either a Tate or Weil pairing (Par [0021]).

Regarding claim 15, Gentry et al '554discloses the method wherein the third private key is combined with a third party's public key to form an associated private key such that an association can be established between the third public key of the second party and the first public key of the first party (Par [0022], Claim 6,12).

Regarding claim 16, Gentry et al '554discloses the method wherein the third private key is a random number (Par [0022], Claim 6,12; random integer/ number).

Regarding claim 17, Gentry et al '554discloses the method wherein the first party is a first trusted party and the second party is a second trusted party (Par [0003], [0004]; trusted party).

Regarding claim 20-21 and 23-24, they recite the limitations of claims 4-5 and 19, therefore, they are rejected applying as above rejecting claims 4-5 and 19.

Conclusion


8. **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin
Examiner, AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


9117107